Framework Gestión de la seguridad de la información para universidades

Integrantes: Maher Herrera Olivares, Isaac Palacio Salcedo, Alison Rada Martínez.

Tutores: Ricardo Luis Villanueva Polanco, Wilson Nieto Bernal.

El gobierno y gestión de los procesos de TI se ven afectados por muchas variables, y la medida de estas es crucial para identificar las posibles vulnerabilidades en los procesos. El estado colombiano reconoce que la información es un recurso y activo que tiene valor y debe ser debidamente protegida (Arevalo, Bayona & Rico, 2015).

Para generar valor desde TI se debe medir el desempeño de los procesos de seguridad y sus riesgos. Para hacer esto se necesitan unos estándares de referencia, como los son el ISO 27000. Los requisitos de esta norma aporta un Sistema de Gestión de la Seguridad de la Información (SGSI) consistente en medidas orientadas a proteger la información, independiente de su formato contra cualquier amenaza, de forma que se garantice la continuidad de las actividades de la empresa (Alemán & Rodríguez, 2018).

Se propone un framework para la gestión de la seguridad en contextos universitarios basado en las Normas ISO 27000. Para esto se elabora una revisión sistemática de la literatura relacionada con Frameworks de seguridad de la información organizacional, se diseña un prototipo para medir el nivel de madurez de un sistema. Y finalmente se valida el marco de trabajo propuesto en un contexto como la Universidad del Norte.

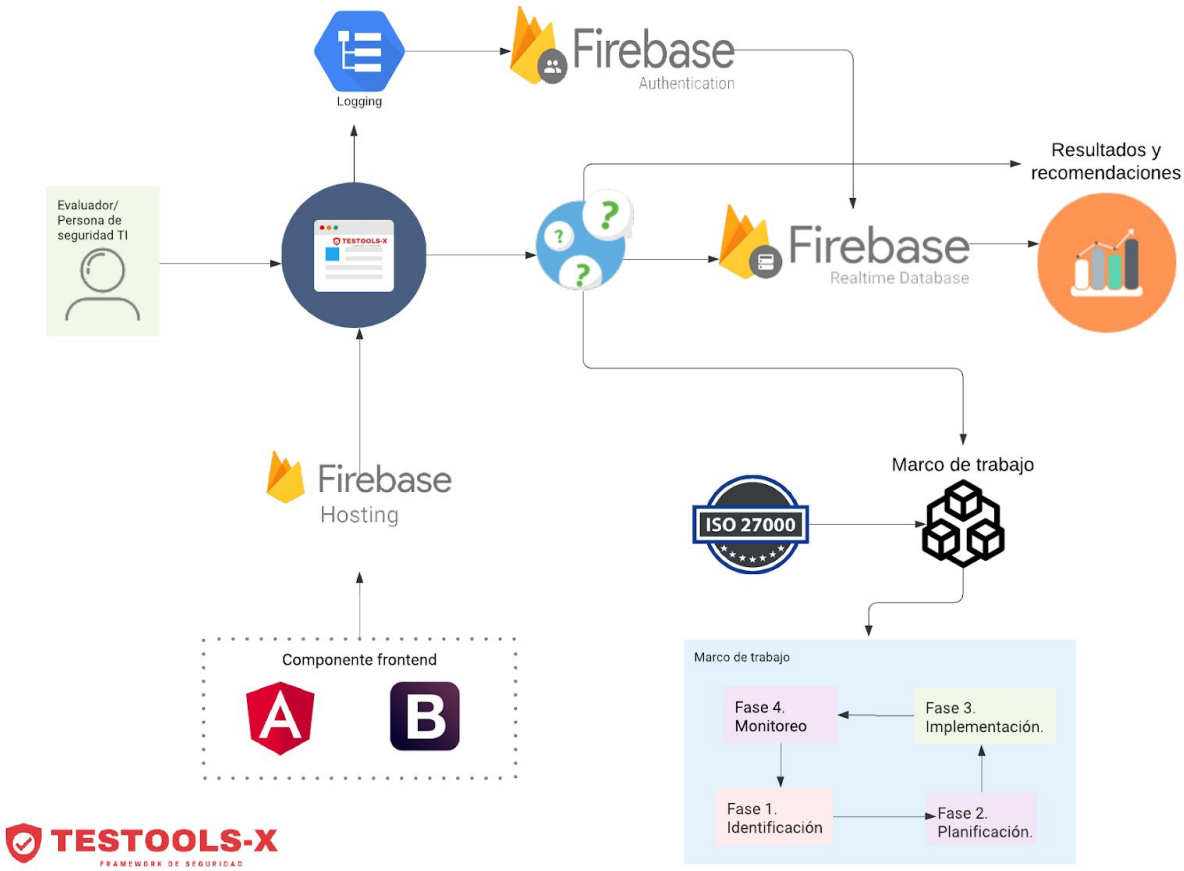
El framework se divide en cuatro fases: primero, se identifica el estado de cumplimiento de los controles en el sistema a evaluar con el uso de la herramienta web diseñada. Segundo, la directiva debe definir un plan de implementación de acuerdo a los riesgos encontrados en la fase anterior. Tercero, se lleva a cabo la ejecución de lo planificado. Y por último, se hace un monitoreo para controlar el desarrollo del funcionamiento de lo implementado, además, en esta fase ha de planificarse la ejecución de las auditorías internas y las revisiones por la dirección.

Referencias

H. Alemán Novoa and C. Rodríguez Barrera, “Metodologías para el análisis de riesgos en los sgsi,” Publicaciones e Investig., vol. 9, p. 73, Oct. 2015, doi: 10.22490/25394088.1435. 2018

J. G. Arévalo Ascanio, R. A. Bayona Trillos, and D. W. Rico Bautista, “Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información,” Rev. Tecnura, vol. 19, no. 46, p. 123, Nov. 2015.

Arquitectura de la solución



TESTOOLS-X
FRAMEWORK DE SEGURIDAD

Information security management framework for universities

Members: Maher Herrera Olivares, Isaac Palacio Salcedo, Alison Rada Martínez.

Tutors: Ricardo Luis Villanueva Polanco, Wilson Nieto Bernal.

Governance and management of IT processes are affected by many variables, and the measurement of these is crucial to identify potential vulnerabilities in the processes. Colombian government recognizes that information is a resource and asset that has value and must be protected properly (Arevalo, Bayona & Rico, 2015).

Strategic IT alignment with the organization is key to the timely implementation of changes. To generate value from IT, the performance of security processes and their risks must be measured. To do this, reference standards are required, such as ISO 27000. The requirements of this standard provide an Information Security Management System (ISMS) consisting of measures aimed at protecting information, regardless of its format against any threat, to guarantee the continuity of the company's activities (Alemán & Rodríguez, 2018).

In a university context, a framework for the management of security based on the ISO 27000 Standards is proposed. For this, a systematic review of the literature related to Frameworks of organizational information security is rendered, a prototype is designed to measure the level of maturity of a system. And finally, the proposed framework is validated in a context such as the Universidad del Norte.

The framework consists of four phases: first, the compliance status of the controls in the system to be evaluated is identified with the use of the designed web tool. Second, the organization directive must define an implementation plan according to the risks found in the previous phase. Third, the execution of what is planned is carried out. And finally, monitoring is carried out to control the development of the operation of what has been implemented, in addition, at this stage the execution of internal audits and management reviews must be planned.

Keywords— ISO 27000, security controls, security assurance, risks, threats, information security, incident management, decision-making, test, monitoring.

References

H. Alemán Novoa and C. Rodríguez Barrera, “Metodologías para el análisis de riesgos en los sgsi,” Publicaciones e Investig., vol. 9, p. 73, Oct. 2015, doi: 10.22490/25394088.1435. 2018

J. G. Arévalo Ascanio, R. A. Bayona Trillos, and D. W. Rico Bautista, “Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información,” Rev. Tecnura, vol. 19, no. 46, p. 123, Nov. 2015.

Solution architecture